involve
a journal of mathematics

The probability of relatively prime polynomials in $\mathbb{Z}_{p^k}[x]$

Thomas R. Hagedorn and Jeffrey Hatley

mathematical sciences publishers

2010 vol. 3, no. 2

INVOLVE 3:2(2010)

The probability of relatively prime polynomials in $\mathbb{Z}_{p^k}[x]$

Thomas R. Hagedorn and Jeffrey Hatley

(Communicated by Arthur T. Benjamin)

Let $\mathrm{P}_R(m, n)$ denote the probability that two randomly chosen monic polynomials $f, g \in R[x]$ of degrees m and n, respectively, are relatively prime. Let $q = p^k$ be a prime power. We establish an explicit formula for $\mathrm{P}_R(m, 2)$ when $R = \mathbb{Z}_q$, the ring of integers mod q.

1. Introduction

Given two polynomials $f(x)$, $g(x)$ chosen at random, what is the probability that they are relatively prime? For a ring R, we say that two polynomials $f, g \in R[x]$ are relatively prime if there is no monic polynomial of positive degree that divides both f and g. Let $\mathrm{P}_R(m, n)$ denote the probability that two randomly chosen monic polynomials $f, g \in R[x]$ of degrees m and n, respectively, are relatively prime. If R has an infinite number of elements, then $\mathrm{P}_R(m, n) = 1$, so we restrict our attention to finite rings R. Let $R = \mathbb{F}_q$, the finite field with q elements. The formula, $\mathrm{P}_{\mathbb{F}_q}(m, m) = 1 - 1/q$ was proved in [Corteel et al. 1998]. When $q = p = 2$, Reifegerste [2000] gave a combinatorial proof that $\mathrm{P}_{\mathbb{F}_2}(m, m) = 1/2$. Benjamin and Bennett subsequently found a beautifully simple proof generalizing these results:

Theorem 1.1 [Benjamin and Bennett 2007]. *If* $m, n \geq 1$, *then* $\mathrm{P}_{\mathbb{F}_q}(m, n) = 1 - \dfrac{1}{q}$.

This can be generalized in at least two ways. Hou and Mullen [2009] have generalized Theorem 1.1 by considering the problem of relatively prime polynomials in several variables over a finite field. In earlier work, Gao and Panario [2006] considered the probability distribution of the greatest common divisor of l randomly chosen monic single-variable polynomials in $\mathbb{F}_q[x]$ with degrees $n_1, \ldots, n_l$ as the $n_i \to \infty$. In this paper, we restrict ourselves to single-variable polynomials and explore a different perspective.

MSC2000: 11C20, 13B25, 13F20.
Keywords: relatively prime polynomials.
The authors would like to thank The College of New Jersey for its support of undergraduate research.

As the formula in Theorem 1.1 only depends on the number of elements in the field $\mathbb{F}_q$, one can ask whether the same formula holds when R is another ring with q elements. For example, if $R = \mathbb{Z}_q$, the integers mod q, does the same formula hold? It does not, but the formula for $\mathrm{P}_{\mathbb{F}_q}(m,n)$ can be viewed as a first approximation to the formula for $\mathrm{P}_{\mathbb{Z}_q}(m,n)$. In this paper, we prove an explicit formula for $\mathrm{P}_{\mathbb{Z}_{p^k}}(m,2)$ for p odd.

For each positive integer k, we define a monic polynomial $f_k(x) \in \frac{1}{2}\mathbb{Z}[x]$ by

$$f_k(x) = x^{2k} + (1-x)\sum_{i=0}^{(k-3)/2} x^{(k+3)/2+3i} + \frac{1}{2}\sum_{i=0}^{k-1}(-x)^i + \tfrac{1}{2}x^{(k-1)/2} - 1,$$

for k odd, and

$$f_k(x) = x^{2k} + (1-x)\sum_{i=1}^{k/2-1} x^{2k-3i} - \frac{1}{2}\sum_{i=1}^{k-1}(-x)^i - x^{k/2+1} + \tfrac{3}{2}x^{k/2} - 1,$$

for k even. The polynomial $f_k(x)$ has degree $2k$ and its coefficients have absolute value at most 2.

Theorem 1.2. *Let p be an odd prime and let $m, k \geq 1$ be integers. The probability that two randomly chosen monic polynomials in $\mathbb{Z}_{p^k}[x]$ of degrees m and 2, respectively, are relatively prime is*

$$\mathrm{P}_{\mathbb{Z}_{p^k}}(m,2) = 1 - \frac{1}{p^{3k}} f_k(p).$$

When $k = 1$, we rediscover $\mathrm{P}_{\mathbb{F}_p}(m,2) = 1 - 1/p$. For small values of k, we have

$$\begin{aligned}
\mathrm{P}_{\mathbb{Z}_{p^2}}(m,2) &= 1 - \frac{1}{p^2} + \frac{1}{p^4} - \frac{2}{p^5} + \frac{1}{p^6},\\
\mathrm{P}_{\mathbb{Z}_{p^3}}(m,2) &= 1 - \frac{1}{p^3} + \frac{1}{p^5} - \frac{1}{p^6} - \frac{1}{2p^7} + \frac{1}{2p^9},\\
\mathrm{P}_{\mathbb{Z}_{p^4}}(m,2) &= 1 - \frac{1}{p^4} + \frac{1}{p^6} - \frac{1}{p^7} + \frac{1}{2p^9} - \frac{1}{p^{10}} - \frac{1}{2p^{11}} + \frac{1}{p^{12}}.
\end{aligned}$$

As an immediate corollary to Theorem 1.2, we obtain:

Corollary 1.3. *Given $k \geq 1$, there exists a monic polynomial*

$$g_k(x) = \sum a_i x^i \in \tfrac{1}{2}\mathbb{Z}[x]$$

with degree $2k-2$ and $|a_i| \leq 2$, such that

$$\mathrm{P}_{\mathbb{Z}_{p^k}}(m,2) = 1 - \frac{1}{p^k} + \frac{1}{p^{3k}} g_k(p) \quad \text{for all odd primes } p \text{ and all } m \geq 1.$$

We obtain Theorem 1.2 and its corollary by adapting the arguments of Benjamin and Bennett [2007], who proved Theorem 1.1 by a clever use of the Euclidean algorithm in $\mathbb{F}_q[x]$. While $\mathbb{Z}_{p^k}[x]$ does not have the Euclidean algorithm, due to the existence of noninvertible elements in $\mathbb{Z}_{p^k}$, it does have a division algorithm for monic polynomials. This division algorithm, together with some facts about polynomial factorization of quadratics in $\mathbb{Z}_{p^k}[x]$, suffices to prove Theorem 1.2 for odd primes p. It appears that our arguments can also be used to prove the formula for $\mathrm{P}_{\mathbb{Z}_{p^k}}(m,2)$ when $p=2$, and also a formula for $\mathrm{P}_{\mathbb{Z}_{p^k}}(m,3)$, but the details are much more involved and have not yet been fully worked through. However, the present approach does not seem able to establish a formula for $\mathrm{P}_{\mathbb{Z}_{p^k}}(m,n)$ for general $m,n \geq 4$ as the number of cases to consider in the proof grows as a function of $\min(m,n)$.

2. Arithmetic in $\mathbb{Z}_{p^k}[x]$

In this section, we establish some basic results on the rings $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_{p^k}[x]$. Recall that $\mathbb{Z}_n$ denotes the ring of integers mod n. We will make use of Hensel's lemma [Gouvêa 1997, page 70] in the following form:

Lemma 2.1 (Hensel's lemma). *Let $f(x) \in \mathbb{Z}_{p^k}[x]$ be a polynomial and denote its reduction mod p by $\bar{f}(x) \in \mathbb{Z}_p[x]$. Suppose there exists $u_0 \in \mathbb{Z}_p$ with $\bar{f}(u_0)=0$ in $\mathbb{Z}_p$ and $\bar{f}'(u_0) \neq 0$ in $\mathbb{Z}_p$. Then there exists a unique $u \in \mathbb{Z}_{p^k}$, with $f(u)=0$ in $\mathbb{Z}_{p^k}$ and $u \equiv u_0 \bmod p$.*

We start by counting the squares in $\mathbb{Z}_{p^k}$ and its unit subgroup $\mathbb{Z}^*_{p^k}$.

Lemma 2.2. *Let p be an odd prime and $k \geq 1$.*

(a) *$\mathbb{Z}^*_{p^k}$ has $\frac{1}{2}p^{k-1}(p-1)$ squares.*

(b) *Let d be even, with $0 \leq d < k$. There are $\frac{1}{2}(p-1)p^{k-1-d}$ nonzero squares $x \in \mathbb{Z}_{p^k}$ with $x \in p^d\mathbb{Z}_{p^k} \setminus p^{d+1}\mathbb{Z}_{p^k}$.*

(c) *There are $1+\dfrac{1}{2(p+1)}(p^{k+1}-p^{1-k+2[k/2]})$ squares in $\mathbb{Z}_{p^k}$.*

Proof. (a) We first note that the $(p-1)/2$ squares $x=1^2,\dots,(\frac{p-1}{2})^2$ are distinct nonzero squares in both $\mathbb{Z}_p$ and $\mathbb{Z}_{p^k}$. Now consider a unit $u \in \mathbb{Z}_{p^k}$ satisfying $u \equiv 1 \bmod p$. Letting $f(x)=x^2-u \in \mathbb{Z}_{p^k}[x]$, and $u_0=1$, by Lemma 2.1, u is a square in $\mathbb{Z}_{p^k}$. Thus the p^{k-1} units $u \in \mathbb{Z}_{p^k}$ with $u \equiv 1 \bmod p$ are squares. Hence, the $\frac{1}{2}p^{k-1}(p-1)$ distinct units xu are all squares and every unit square can be seen to be of this form.

(b) Let $x \in \mathbb{Z}_{p^k}$ satisfy $x \in p^d\mathbb{Z}_{p^k} \setminus p^{d+1}\mathbb{Z}_{p^k}$. Let $x=(p^tu)^2=p^{2t}u^2$, where u is a unit. To satisfy the given conditions, $t=d/2$, u^2 is a unit square in $\mathbb{Z}^*_{p^k}$, and $u^2 \equiv u_1^2 \bmod p^{k-d}$. Hence, the number of distinct x equals the number of unit squares in $\mathbb{Z}_{p^{k-d}}$, which is given by (a).

(c) Every nonzero square can be written as $p^{2d}u$, where u is a unit square and $0 \le 2d < n$. Counting the square 0, the total sum is, thanks to (b),

$$1+\tfrac{1}{2}(p-1)\sum_{d=0}^{[(k-1)/2]} p^{k-1-2d}.$$

This expression simplifies to the claimed formula. □

For $g(x) = x^2 + bx + c \in \mathbb{Z}_{p^k}[x]$, define the discriminant $\Delta_g = b^2 - 4c$. As when $k = 1$, we can describe the number of roots of $g(x) \in \mathbb{Z}_{p^k}[x]$ using Δ_g.

Lemma 2.3. *Let p be an odd prime, $k \ge 1$, and $g(x) = x^2 + bx + c \in \mathbb{Z}_{p^k}[x]$.*

(a) *Δ is a square mod p^k if and only if g is reducible.*

(b) *If $\Delta \equiv 0 \bmod p^k$, then g has the $p^{[k/2]}$ roots given by $\dfrac{-b}{2} + p^{[(k+1)/2]}t \bmod p^k$, where $t = 1, \ldots, p^{[k/2]}$.*

(c) *Suppose $\Delta \equiv p^d u \bmod p^k$ is a nonzero square with $0 \le d < k$, d even, $u \in \mathbb{Z}^*_{p^k}$ a square. Choose a such that $u \equiv a^2 \bmod p^k$. Then g has the $2p^{d/2}$ roots*

$$-\tfrac{1}{2}b \pm \tfrac{1}{2}ap^{d/2} + tp^{k-d/2} \mod p^k, \qquad \textit{where } t = 1, \ldots, p^{d/2}.$$

Proof. Since p is odd, we have $g(x) = (x+b/2)^2 - \Delta/4$. Hence $r = -(b+z)/2$ is a root of $g(x)$ if and only if z is a solution of the equation $z^2 \equiv \Delta \bmod p^k$. Condition (a) is thus proved. Condition (b) follows as well as the roots of the equation $z^2 \equiv 0 \bmod p^k$ are $z \equiv p^{[(k+1)/2]}t \bmod p^k$, for $t = 1, \ldots, p^{[k/2]}$, or equivalently, $z \equiv 2p^{[(k+1)/2]}t \bmod p^k$, for $t = 1, \ldots, p^{[k/2]}$. (c) By the hypothesis, d is even and $a \not\equiv 0 \bmod p$. The solutions to the equation $z^2 \equiv p^d a^2 \bmod p^k$ have the form $z \equiv p^{d/2}w \bmod p^k$, where $w \in \mathbb{Z}_{p^k}$ is a solution of $x^2 \equiv a^2 \bmod p^{k-d}$. Hensel's lemma (using the polynomial $f(x) = x^2 - a^2$), shows that the solutions to this latter equation are the $w \in \mathbb{Z}_{p^k}$ satisfying $w \equiv \pm a \bmod p^{k-d}$. Thus $w = \pm a + tp^{k-d}$, for $t = 1, \ldots, p^d$, or equivalently, as 2 is a unit mod p^d, $w = \pm a + 2tp^{k-d}$ for $t = 1, \ldots, p^d$. Now two roots $z = p^{d/2}w$ and $z_1 = p^{d/2}w_1$ are equal precisely when the signs in the expressions for w and w_1 agree and the respective parameters t and t_1 satisfy $t \equiv t_1 \bmod p^{d/2}$. Hence we have shown that the original equation $z^2 \equiv p^d a^2 \bmod p^k$ has the $2p^{d/2}$ distinct roots given by $z = \pm ap^{d/2} + 2tp^{k-d/2}$, for $t = 1, \ldots, p^{d/2}$. □

Lemma 2.4. *Let p be an odd prime and $k \ge 1$.*

(a) *Given $\Delta \in \mathbb{Z}_{p^k}$, there are p^k monic, quadratic polynomials $g \in \mathbb{Z}_{p^k}[x]$ with $\Delta_g \equiv \Delta \bmod p^k$.*

(b) *There are*

$$\frac{p^k}{2(p+1)}(p^{k+1}+2p^k-p-p^{k-2[k/2]}-1)$$

monic, irreducible, quadratic polynomials $g \in \mathbb{Z}_{p^k}[x]$.

Proof. If $g = x^2+bx+c$, then $\Delta_g = b^2-4c$. Since 4 is invertible mod p^k, for every Δ, $b \in \mathbb{Z}_{p^k}$, there is a unique choice of c such that $\Delta_g \equiv \Delta \bmod p^k$. Since there are p^k choices for b, (a) is proved. Now g is irreducible precisely when Δ_g is not a square. Let S be the number of squares in $\mathbb{Z}_{p^k}$. Then for each $b \in \mathbb{Z}_{p^k}$, there are $p^k - S$ choices for c such that b^2-4c is not a square. Thus, using the formula for S given by Lemma 2.2(c), there are

$$p^k(p^k-S) = \frac{p^k}{2(p+1)}\big(p^{k+1}+2p^k-2p+p^{1-k+2[k/2]}-2\big)$$

irreducible polynomials g. Simplification gives (b). □

Given a monic, quadratic polynomial $g \in \mathbb{Z}_{p^k}[x]$, we define the set

$$A_g = \{h \in \mathbb{Z}_{p^k}[x] : \deg h \le 1 \text{ and } g, h \text{ are not relatively prime}\},$$

and let $|A_g|$ denote its cardinality. We note that in the definition of A_g, we allow nonmonic polynomials h.

Lemma 2.5. *Let p be an odd prime and $g(x)$ be a monic quadratic polynomial in* $\mathbb{Z}_{p^k}[x]$.

(a) *If* $\Delta_g \equiv 0 \bmod p^k$, *then*

$$|A_g| = p^{k-[k/2]}\left(\frac{p^{2[k/2]+1}+1}{p+1}\right).$$

(b) *Assume $\Delta_g \in \mathbb{Z}_{p^k}$ is a nonzero square. Let $\Delta_g \equiv p^d v \bmod p^k$, where d is even, $0 \le d < k$, and $v \in (\mathbb{Z}^*_{p^k})^2$. Then*

$$|A_g| = 2p^{k-d/2}\left(\frac{p^{d+1}+1}{p+1}\right) - p^{d/2}.$$

Proof. We first note that a linear factor of $g(x)$ must have the form $u(x-r)$, where $u, r \in \mathbb{Z}_{p^k}$, u is a unit, and r is a root of g. Therefore, the elements $h(x) \in A_g$ are exactly the polynomials $h(x) = \alpha(x-r)$, for some $\alpha \in \mathbb{Z}_{p^k}$ and some root $r \in \mathbb{Z}_{p^k}$ of g. Hence, to calculate $|A_g|$, we need to count the number of distinct $h(x)$ of this form.

Suppose r_1 and r_2 are two roots of g and $\alpha(x-r_1) \equiv \beta(x-r_2) \bmod p^k$. Then $\beta \equiv \alpha \bmod p^k$ and $\alpha(r_1-r_2) \equiv 0 \bmod p^k$. Let $\alpha = p^s u$, with $u \in \mathbb{Z}^*_{p^k}$. If $s = k$, then $\alpha = 0$ is the only choice. Now suppose $s < k$. Then there are $p^{k-s-1}(p-1)$ distinct choices for u giving rise to distinct α. For each such α, we need to calculate the number of roots of g in $\mathbb{Z}_{p^{k-s}}$. To proceed further, we need to have a description of the roots.

Writing $g(x) = x^2 + bx + c$, in case (a), the roots of g are $r = -b/2 + p^{[(k+1)/2]}t$, for $t = 1, \dots, p^{[k/2]}$ by Lemma 2.3. If $[k/2] \le s < k$, for each choice of $\alpha = p^s u$, there is exactly one factor $\alpha(x-r) \bmod p^k$. As there are $p^{k-s-1}(p-1)$ choices for u, and hence α, we obtain the same number of distinct factors $\alpha(x-r)$ for each s. If $0 \le s \le [k/2]$, then for each choice of $\alpha = p^s u$, there are $p^{[k/2]-s}$ distinct factors $\alpha(x-r) \bmod p^k$. Hence there are $p^{k+[k/2]-2s-1}(p-1)$ distinct factors $\alpha(x-r) \bmod p^k$ for each s. In total then, we have

$$
\begin{aligned}
|A_g| &= \sum_{s=0}^{[k/2]} (p-1)p^{k+[k/2]-2s-1} + \left(\sum_{s=[k/2]+1}^{k-1} (p-1)p^{k-s-1} + 1 \right) \\
&= \sum_{s=0}^{[k/2]} (p-1)p^{k+[k/2]-2s-1} + p^{k-[k/2]-1} = p^{k-[k/2]} \left(\frac{p^{2[k/2]+1}+1}{p+1} \right),
\end{aligned}
$$

where the last equality is obtained by evaluating a geometric sum. We thus obtain the desired formula for case (a). In case (b), by Lemma 2.3, the roots of g are $-\frac{1}{2}b \pm \frac{1}{2}ap^{d/2} + tp^{k-d/2} \bmod p^k$, where $a^2 \equiv v \bmod p^k$, $t = 1, \dots, p^{d/2}$. As in case (a), we let $\alpha = p^s u$, and consider the number of distinct factors $h(x) = \alpha(x-r)$ for each choice of s. When $s = k$, $h(x) = \alpha = 0$ is the only factor. There are three additional cases:

(1) Suppose $k > s \ge k - d/2$. Then $k - s \le d/2$ and all the roots of g are equivalent mod p^{k-s}. Since there are $p^{k-s-1}(p-1)$ distinct choices for α, there are the same number of distinct factors $\alpha(x-r)$.

(2) Suppose $k - d/2 > s \ge d/2$. Then $d/2 < k - s \le k - d/2$ and the roots of g determine two equivalence classes mod p^{k-s}. Thus for each s, there are a total of $2p^{k-s-1}(p-1)$ distinct factors $\alpha(x-r)$.

(3) Suppose $d/2 \ge s \ge 0$. Then the roots of g determine $2p^{d/2-s}$ equivalence classes mod p^{k-s} for each α. Thus there are a total of $2p^{k+d/2-2s-1}(p-1)$ distinct factors $\alpha(x-r)$, for each s.

In total, when $d < k-1$, we have for $|A_g|$ the value

$$
\begin{aligned}
&\sum_{s=0}^{d/2} 2(p-1)p^{k+d/2-2s-1} + \left(\sum_{s=d/2+1}^{k-d/2-1} 2(p-1)p^{k-s-1} + \sum_{s=k-d/2}^{k-1} (p-1)p^{k-s-1} + 1 \right) \\
&\qquad = \sum_{s=0}^{d/2} 2(p-1)p^{k+d/2-2s-1} + 2p^{k-d/2-1} - p^{d/2},
\end{aligned}
$$

which simplifies to the formula stated in (b). When $d=k-1$, the second summation does not appear, and

$$\begin{aligned}|A_g| &= \sum_{s=0}^{d/2} 2(p-1)p^{k+d/2-2s-1} + \Bigg(\sum_{s=k-d/2}^{k-1}(p-1)p^{k-s-1}+1\Bigg)\\ &= \sum_{s=0}^{d/2} 2(p-1)p^{k+d/2-2s-1} + p^{d/2},\end{aligned}$$

which again simplifies to the stated formula for (b). □

3. Proof of the main theorem

In this section, we let $q = p^k$. To prove Theorem 1.2, we will count the number of polynomial pairs (f, g), where $f, g \in \mathbb{Z}_q[x]$ are not relatively prime. Let $f(x)$, $g(x)$ be monic polynomials. Then by the division algorithm, there is a unique choice of polynomials $q(x), r(x) \in \mathbb{Z}_q[x]$, with $q(x)$ monic, satisfying

$$f(x) = g(x)q(x) + r(x), \tag{1}$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Thus the pair (f, g) is uniquely determined by the triple $(g, q(x), r(x))$. From (1), any common divisor of f and g is a common divisor of g and r and vice-versa. We define

$$\begin{aligned}S_{m,d,q} &= \{(f, g) : f, g \in \mathbb{Z}_q[x] \text{ monic with } \deg f = m,\ \deg g = d,\\ &\qquad\qquad f \text{ and } g \text{ not relatively prime}\},\\ T_{m,q} &= \{(g, r) : g, r \in \mathbb{Z}_q[x] \text{ with } g \text{ monic of degree } m,\ \deg r < m,\\ &\qquad\qquad g \text{ and } r \text{ not relatively prime}\}.\end{aligned}$$

Lemma 3.1. *If $m \geq d$, then $|S_{m,d,q}| = q^{m-d}|T_{d,q}|$.*

Proof. Let $(g, r) \in T_{d,q}$. Then each of the q^{m-d} monic polynomials $q(x)$ with degree $m-d$ gives rise via (1) to a unique pair $(f, g) \in S_{m,d,q}$. Conversely, the inverse map

$$(f, g) \mapsto (g, q, r) \mapsto (g, r)$$

is a q^{m-d}-to-1 map from $S_{m,d,q}$ to $T_{d,q}$. □

Thus, proving Theorem 1.2 is reduced to calculating $|T_{2,q}|$. We begin with:

Proposition 3.2. $|T_{1,q}| = q$.

Proof. If $(g, r) \in T_{1,q}$, then $g(x) = x - c$. For g and r to have a common factor, $r = 0$. Hence $T_{1,q}$ consists of the q pairs $(x - c, 0)$. □

We now determine $|T_{2,q}|$. By Lemma 2.3, we have $|T_{2,q}| = B_1 + B_2 + B_3$, where the B_i are defined by

$$B_1 = \big|\{(g,r) \in T_{2,q} : g \text{ is irreducible}\}\big|,$$

$$B_2 = \big|\{(g,r) \in T_{2,q} : \Delta_g \equiv 0 \bmod p^k\}\big|,$$

$$B_3 = \big|\{(g,r) \in T_{2,q} : \Delta_g \bmod p^k \text{ is a square, and, for each } d < k, \\ \Delta_g \equiv 0 \bmod p^d \text{ and } \Delta_g \not\equiv 0 \bmod p^{d+1}\}\big|.$$

Lemma 3.3. (a) $B_1 = \dfrac{p^k}{2(p+1)}(p^{k+1} + 2p^k - p - p^{k-2[k/2]} - 1)$.

(b) $B_2 = p^{2k-[k/2]}\left(\dfrac{p^{2[k/2]+1}+1}{p+1}\right)$.

(c) $B_3 = \dfrac{p^{2k-1-[(k-1)/2]} - p^{2k}}{2(p+1)(p^2+p+1)}\alpha$, *where*

$$\alpha = (p+1)(p^2+p+1) - 2p^{k+1}(p+1)^2 - 2p^{k-[(k-1)/2]}(p + p^{-[(k-1)/2]}).$$

Proof. (a) Assume $g \in \mathbb{Z}_{p^k}[x]$ is a monic, irreducible, quadratic polynomial. Since g has no factors, $(g,r) \in T_{2,q}$ only when $r = 0$. Hence, B_1 equals the number of monic, irreducible quadratic polynomials, which is given by Lemma 2.4.

(b) Assume $g \in \mathbb{Z}_{p^k}[x]$ is a monic quadratic with $\Delta_g \equiv 0 \bmod p^k$. By Lemma 2.4, there are p^k such g. For each g, $|A_g|$ is given by Lemma 2.5(a). Thus

$$B_2 = p^k|A_g|.$$

(c) If $(g,r) \in T_{2,q}$ is included in the pairs counted for B_3, then $\Delta_g = p^d u$, where $0 \le d < k$, d even, and $u \in \mathbb{Z}^*_{p^k}$ is a square. For a fixed d, u, satisfying these conditions, there are p^k polynomials g with $\Delta_g = p^d u$ by Lemma 2.4(a). And for any such g, $|A_g|$ is given by Lemma 2.5(b). Now, for a fixed d, there are

$$\tfrac{1}{2}(p-1)p^{k-d-1}$$

choices for u that give distinct values for $p^d u$. Putting these results together, and replacing d by $2d$, we have

$$\begin{aligned} B_3 &= \sum_{d=0}^{[(k-1)/2]} \frac{1}{2}(p-1)p^{2k-d-1}\left(2p^{k-2d}\left(\frac{p^{2d+1}+1}{p+1}\right) - 1\right) \\ &= \frac{p^{2k-1}(p-1)}{2(p+1)} \sum_{d=0}^{[(k-1)/2]} p^{-d}\big(2p^{k-2d}(p^{2d+1}+1) - p - 1\big). \end{aligned} \tag{2}$$

Summing the geometric sequences, we have

$$\sum_{d=0}^{[(k-1)/2]} p^{-d}(-p-1) = -(p+1)p^{-[(k-1)/2]}\Big(\frac{p^{[(k-1)/2]+1}-1}{p-1}\Big),$$

$$\sum_{d=0}^{[(k-1)/2]} p^{-d}\big(2p^{k-2d}(p^{2d+1}+1)\big) = 2p^{k-[(k-1)/2]+1}\Big(\frac{p^{[(k-1)/2]+1}-1}{p-1}\Big) +2p^{k-3[(k-1)/2]}\Big(\frac{p^{3[(k-1)/2]+3}-1}{p^3-1}\Big).$$

Substituting these equations in (2) and simplifying with the help of a computer algebra system, we obtain the desired expression. □

Proof of Theorem 1.2. There are q^m monic polynomials in $\mathbb{Z}_q[x]$ with degree m. Hence there are q^{m+2} pairs of monic polynomials (f, g) with $\deg f = m$, $\deg g = 2$. By Lemma 3.1, the probability that a pair of these polynomials is relatively prime is

$$1-\frac{|S_{m,2,q}|}{q^{m+2}} = 1-\frac{|T_{2,q}|}{q^4}.$$

Now $|T_{2,q}| = B_1+B_2+B_3$, with the values of B_i given by Lemma 2.5. Manipulating this expression with the help of a computer algebra system, one obtains

$$|T_{2,q}| = \frac{p^k}{2(p+1)}D,$$

where D equals the expression

$$2p^{2k+1}+2p^{2+k/2}(p-1)\Big(\frac{p^{3k/2}-1}{p^3-1}\Big)+p^{1+k/2}+3p^{k/2}+p^k-p-2$$

when k is even, and D equals

$$2p^{2k+1}+2(p-1)\Big(\frac{p^{2(k+1)}-p^{(k+1)/2}}{p^3-1}\Big)+3p^{(k+1)/2}+p^{(k-1)/2}+p^k-2p-1,$$

when k is odd. When k is even, algebraic manipulation shows

$$2p^{2k+1} = 2(p+1)p^{2k}-2p^{2k},$$

$$2p^{2+k/2}(p-1)\Big(\frac{p^{3k/2}-1}{p^3-1}\Big) = 2p^{2k}-2p^{2+k/2}+2(1-p^2)\sum_{i=1}^{k/2-1} p^{2k-3i},$$

$$p^{1+k/2}+3p^{k/2} = (p+1)(-2p^{1+k/2}+3p^{k/2})+2p^{2+k/2},$$

$$p^k-p-2 = -(p+1)\sum_{i=1}^{k-1}(-p)^i-2(p+1).$$

Adding both sides, the left hand side sums to D. With $f_k(x)$ defined as in the introduction, we then have

$$\frac{1}{2(p+1)} D = f_k(p).$$

Theorem 1.2 follows immediately for k even. Similar calculations establish it for k odd. □

Acknowledgment

The authors thank the anonymous referee for many helpful suggestions.

References

[Benjamin and Bennett 2007] A. T. Benjamin and C. D. Bennett, "The probability of relatively prime polynomials", *Math. Mag.* **80**:3 (2007), 196–202. MR 2008b:11036

[Corteel et al. 1998] S. Corteel, C. D. Savage, H. S. Wilf, and D. Zeilberger, "A pentagonal number sieve", *J. Combin. Theory Ser. A* **82**:2 (1998), 186–192. MR 99d:11111 Zbl 0910.05008

[Gao and Panario 2006] Z. Gao and D. Panario, "Degree distribution of the greatest common divisor of polynomials over $\mathbb{F}_q$", *Random Structures Algorithms* **29**:1 (2006), 26–37. MR 2008k:60020 Zbl 1099.11072

[Gouvêa 1997] F. Q. Gouvêa, *p-adic numbers*, 2nd ed., Universitext, Springer, Berlin, 1997. MR 98h:11155 Zbl 0874.11002

[Hou and Mullen 2009] X.-D. Hou and G. L. Mullen, "Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields", *Finite Fields Appl.* **15**:3 (2009), 304–331. MR 2010c:11146 Zbl 05554713

[Reifegerste 2000] A. Reifegerste, "On an involution concerning pairs of polynomials over $\mathbf{F}_2$", *J. Combin. Theory Ser. A* **90**:1 (2000), 216–220. MR 2001a:11196 Zbl 1010.11068

Received: 2009-12-11 Revised: 2010-04-25 Accepted: 2010-04-26

hagedorn@tcnj.edu *The College of New Jersey, Department of Mathematics and Statistics, P.O. Box 7718, Ewing, NJ 08628, United States*

hatley@math.umass.edu *The College of New Jersey, Department of Mathematics and Statistics, P.O. Box 7718, Ewing, NJ 08628, United States*

Department of Mathematics and Statistics, University of Massachusetts at Amherst, Amherst, MA 01003

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2010 is US $100/year for the electronic version, and $120/year (+$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2010 vol. 3 no. 2

1944-4176(2010)3:2;1-F